(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－344228
（P2001－344228A）
(43)公開日　平成13年12月14日(2001.12.14)

(51)Int.Cl.[7]		識別記号	Ｆ Ｉ		テーマコード（参考）	
Ｇ０６Ｆ	15/177	６７４	Ｇ０６Ｆ	15/177	６７４Ａ	５Ｂ０４５
Ｈ０４Ｌ	9/10		Ｈ０４Ｌ	9/00	６２１Ｚ	５Ｊ１０４
	12/56			11/20	１０２Ａ	５Ｋ０３０

審査請求　未請求　請求項の数９　ＯＬ　（全 ７ 頁）

(21)出願番号　特願2000－163682(P2000－163682)

(22)出願日　平成12年５月31日(2000.5.31)

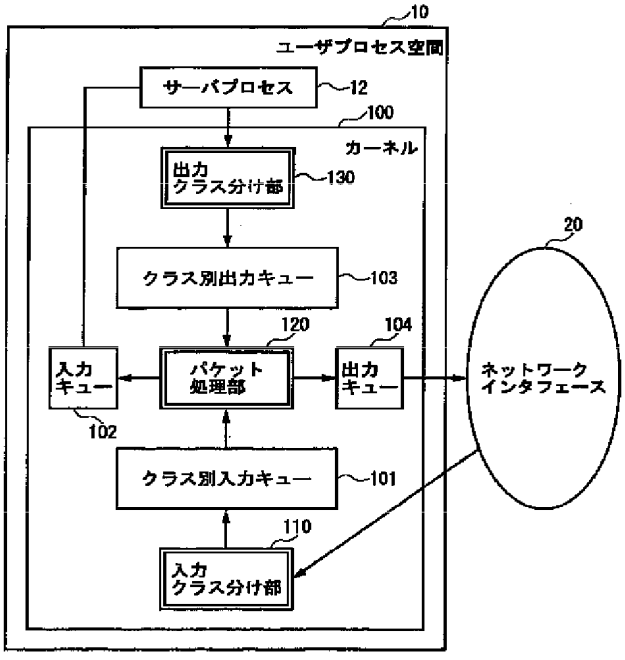
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　本庄　利守
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　小野　諭
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】　暗号化通信におけるサービス品質制御方法及び装置サービス品質制御プログラムを格納した記憶媒体

(57)【要約】
【課題】　暗号化通信を用いたサービスを行う場合に、優先度に応じたサービス品質の制御を正しく行うことが可能な暗号化通信におけるサービス品質制御方法及び装置及びサービス品質制御プログラムを格納した記憶媒体を提供する。
【解決手段】　本発明は、ユーザプロセス空間において、サービスを行うサーバプロセスとカーネル空間において、暗号復号化処理を行うパケット処理のそれぞれに割り当てるＣＰＵ数を制限して、サービスの品質を制御する。

本発明のサービス品質制御装置の構成図



【特許請求の範囲】
【請求項１】　パケットを暗号化することによってセキュアな通信を行う際に、暗号復号化処理をカーネル内で行い、かつ、マルチＣＰＵ及びカーネルにおけるマルチスレッドをサポートしているＯＳを用いて、サービスの品質を保証した通信を行うための暗号化通信におけるサービス品質制御方法において、ユーザプロセス空間において、サービスを行うサーバプロセスとカーネル空間において、暗号復号化処理を行うパケット処理のそれぞれに割り当てるＣＰＵ数を制限して、サービスの品質を制御することを特徴とする暗号化通信におけるサービス品質制御方法。
【請求項２】　パケットをサービスの種類に応じてクラス分けし、それぞれのクラスに割り当てるＣＰＵ数を制御することにより、カーネル内における通信品質を制御する請求項１記載の暗号化通信におけるサービス品質制御方法。
【請求項３】　クラス分けされたパケットのうち、優先度の低いパケットの暗号復号処理を前記ユーザプロセス空間のプロセスによって処理し、通信品質を制御する請求項１または、２記載の暗号化通信におけるサービス品質制御方法。
【請求項４】　パケットを暗号化することによってセキュアな通信を行う際に、暗号復号化処理をカーネル内で行い、かつマルチＣＰＵ及びカーネルにおけるマルチスレッドをサポートしているＯＳを用いて、サービスの品質を保証した通信を行うための暗号化通信におけるサービス品質制御装置であって、ユーザプロセス空間のサービスを行うサーバプロセスとカーネル空間において、暗号復号化処理を行うパケット処理のそれぞれに割り当てるＣＰＵ数を制限して、サービスの品質を制御する制御手段を有することを特徴とする暗号化通信におけるサービス品質制御装置。
【請求項５】　前記制御手段は、パケットをサービスの種類に応じてクラス分けする手段と、それぞれのクラスに割り当てるＣＰＵ数を制御する手段を含む請求項４記載の暗号化通信におけるサービス品質制御装置。
【請求項６】　前記制御手段は、クラス分けされたパケットのうち、優先度の低いパケットの暗号復号処理を前記ユーザプロセス空間のプロセスによって処理し、通信品質を制御する手段を含む請求項４または、５記載の暗号化通信におけるサービス品質制御装置。
【請求項７】　パケットを暗号化することによってセキュアな通信を行う際に、暗号復号化処理をカーネル内で行い、かつマルチＣＰＵ及びカーネルにおけるマルチスレッドをサポートしているＯＳを用いて、サービスの品質を保証した通信を行うためのサービス品質制御プログラムを格納した記憶媒体であって、ユーザプロセス空間のサービスを行うサーバプロセスとカーネル空間において、暗号復号化処理を行うパケット処理のそれぞれに割り当てるＣＰＵ数を制限して、サービスの品質を制御する制御プロセスを有することを特徴とするサービス品質制御プログラムを格納した記憶媒体。
【請求項８】　前記制御プロセスは、パケットをサービスの種類に応じてクラス分けするプロセスと、それぞれのクラスに割り当てるＣＰＵ数を制御するプロセスを含む請求項７記載のサービス品質制御プログラムを格納した記憶媒体。
【請求項９】　前記制御プロセスは、クラス分けされたパケットのうち、優先度の低いパケットの暗号復号処理を前記ユーザプロセス空間のプロセスによって処理し、通信品質を制御するプロセスを含む請求項７または、８記載のサービス品質制御プログラムを格納した記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、暗号化通信におけるサービス品質制御方法及び装置及びサービス品質制御プログラムを格納した記憶媒体に係り、特に、インターネットのようなパケット交換型ネットワークにおいて、ＩＰｓｅｃなどを用いて暗号化通信を行うことにより、セキュアかつ、リアルタイム性などサービス品質を保証した通信サービスを提供する場合に、これらの通信サービスの品質を制御するための暗号化通信におけるサービス品質制御方法及び装置及びサービス品質制御プログラムを格納した記憶媒体に関する。
【０００２】
【従来の技術】従来から、サービス品質を制御する方法として、ネットワークの通信品質を制御する方法及び、ＯＳにおけるサービスプロセスの品質（優先度）を制御する方法の２つが存在する。ネットワークの通信品質を制御する方法として、IntServやDiffServなどがあり、それぞれIntServ は、帯域予約を行う帯域確保型の通信品質制御方式であり、DiffServは、優先制御型の通信品質制御方式である。
【０００３】また、ＯＳにおけるユーザプロセスの品質（優先度）を制御する方法としては、時分割方式や実時間プロセスと時分割プロセスに分けてスケジュールする方式などがある。
【０００４】また、インターネットにおいて、暗号化技術を用いてセキュアな通信を提供する方法として、ＩＰｓｅｃ、ＳＳＬ、ＴＬＳ、Ｓ／ＭＩＭＥなどが挙げられる。それぞれ適用範囲が異なり、それぞれＩＰｓｅｃは、ＩＰ層、ＳＳＬ、ＴＬＳは、Ｔｒａｎｓｐｏｒｔ層、Ｓ／ＭＩＭＥはアプリケーション層（電子メール）である。通常、ＳＳＬ，ＴＬＳ，Ｓ／ＭＩＭＥにおける暗号化処理はユーザプロセス空間で行われる。一方、ＩＰｓｅｃは、通常ＩＰの拡張として導入されるため、ソフトウェアにより実現する場合には、暗号処理もカーネル内で行われる。本発明では、ＩＰｓｅｃのような暗号

通信が対象となる。
【０００５】
【発明が解決しようとする課題】従来、ＯＳにおいて、カーネルは、キーボードやディスクなどのＩ／Ｏバウンドな処理がメインである。通常Ｉ／Ｏバウンドな処理は、軽く短い処理である。しかし、パケット暗号化処理をカーネル内部において行わせることにより、ＣＰＵバウンドな重たい処理をカーネルに行わせることになる。従って、カーネルが長時間ＣＰＵを占有することになる。通常のＯＳでは、カーネルによる処理は、ユーザプロセスによる処理よりも優先させるという特徴がある。また、ＯＳにおける通信サービスは、カーネル内部による通信処理とユーザプロセス空間におけるサーバプロセスの処理の２つから行われる。
【０００６】以上のようなことから、次のような場合に、優先度逆転（Priority Inversion）の問題が発生する。
【０００７】優先度の高いサービスと低いサービスを共に暗号化通信を用いて同時に提供する場合において、優先度の高いサービスのユーザプロセス空間におけるサーバプロセスの処理よりも、優先度の低いサービスのカーネル内部によるパケット処理の方が優先されてしまい、優先度の高いサービスと優先度の低いサービスの品質制御が正しく行われないという問題がある。
【０００８】本発明は、上記の点に鑑みなされたもので、暗号化通信を用いたサービスを行う場合に、優先度に応じたサービス品質の制御を正しく行うことが可能な暗号化通信におけるサービス品質制御方法及び装置及びサービス品質制御プログラムを格納した記憶媒体を提供することを目的とする。
【０００９】
【課題を解決するための手段】本発明（請求項１）は、パケットを暗号化することによってセキュアな通信を行う際に、暗号復号化処理をカーネル内で行い、かつマルチＣＰＵ及びカーネルにおけるマルチスレッドをサポートしているＯＳを用いて、サービスの品質を保証した通信を行うための暗号化通信におけるサービス品質制御方法において、ユーザプロセス空間において、サービスを行うサーバプロセスとカーネル空間において、暗号復号化処理を行うパケット処理のそれぞれに割り当てるＣＰＵ数を制限して、サービスの品質を制御する。
【００１０】本発明（請求項２）は、パケットをサービスの種類に応じてクラス分けし、それぞれのクラスに割り当てるＣＰＵ数を制御することにより、カーネル内における通信品質を制御する。
【００１１】本発明（請求項３）は、クラス分けされたパケットのうち、優先度の低いパケットの暗号復号処理をユーザプロセス空間のプロセスによって処理し、通信品質を制御する。
【００１２】本発明（請求項４）は、パケットを暗号化することによってセキュアな通信を行う際に、暗号復号化処理をカーネル内で行い、かつマルチＣＰＵ及びカーネルにおけるマルチスレッドをサポートしているＯＳを用いて、サービスの品質を保証した通信を行うための暗号化通信におけるサービス品質制御装置であって、ユーザプロセス空間のサービスを行うサーバプロセスとカーネル空間において、暗号復号化処理を行うパケット処理のそれぞれに割り当てるＣＰＵ数を制限して、サービスの品質を制御する制御手段を有する。
【００１３】本発明（請求項５）は、制御手段において、パケットをサービスの種類に応じてクラス分けする手段と、それぞれのクラスに割り当てるＣＰＵ数を制御する手段を含む。
【００１４】本発明（請求項６）は、制御手段において、クラス分けされたパケットのうち、優先度の低いパケットの暗号復号処理をユーザプロセス空間のプロセスによって処理し、通信品質を制御する手段を含む。本発明（請求項７）は、パケットを暗号化することによってセキュアな通信を行う際に、暗号復号化処理をカーネル内で行い、かつマルチＣＰＵ及びカーネルにおけるマルチスレッドをサポートしているＯＳを用いて、サービスの品質を保証した通信を行うためのサービス品質制御プログラムを格納した記憶媒体であって、ユーザプロセス空間のサービスを行うサーバプロセスとカーネル空間において、暗号復号化処理を行うパケット処理のそれぞれに割り当てるＣＰＵ数を制限して、サービスの品質を制御する制御プロセスを有する。
【００１５】本発明（請求項８）は、制御プロセスにおいて、パケットをサービスの種類に応じてクラス分けするプロセスと、それぞれのクラスに割り当てるＣＰＵ数を制御するプロセスを含む。
【００１６】本発明（請求項９）は、制御プロセスにおいて、クラス分けされたパケットのうち、優先度の低いパケットの暗号復号処理をユーザプロセス空間のプロセスによって処理し、通信品質を制御するプロセスを含む。
【００１７】上記のように、本発明は、カーネルにおけるパケット処理とユーザプロセス空間における処理のそれぞれに割り当てるＣＰＵ数を制限することにより、サービスの品質を制御することが可能となる。
【００１８】また、パケットをサービスの種類に応じてクラス分けし、それぞれのクラスに割り当てるＣＰＵ数を制限することにより、カーネル内における通信品質を制御することが可能となる。
【００１９】また、クラス分けされたうち、優先度の低いパケットの暗号・復号処理をユーザプロセス空間のプロセスによって処理することにより、優先度を下げて通信品質を制御することが可能となる。
【００２０】
【発明の実施の形態】図１は、本発明のサービス品質制

御装置の構成を示す。
【００２１】同図に示すサービス品質制御装置は、ネットワークインタフェース２０に接続されるカーネル１００およびサーバプロセス１２を包含するユーザプロセス空間１０により構成される。
【００２２】カーネル１００は、入力クラス分け部１１０、パケット処理部１２０、出力クラス分け部１３０から構成される。同図では、入力クラス分け部１１０と出力クラス分け部１３０を分けて示しているが、１つのクラス分け部として構築してもよい。
【００２３】入力クラス分け部１１０は、ネットワークインタフェース２０から入力されたパケットを優先度に応じてクラス分けし、クラス別入力キュー１０１に設定する。
【００２４】パケット処理部１２０は、クラス別入力キュー１０１または、クラス別出力キー１０３に設定されたキューに入れられたパケットを処理する。パケット処理は、それぞれに割り当てられたＣＰＵ数までの範囲の並列度に基づいて処理を行う。パケット処理のＣＰＵ数の制限方法については後述する。また、場合によっては、ユーザプロセス空間１０の暗号処理プロセスに暗号処理を引き渡し、処理してもらうことも可能である。
【００２５】出力クラス分け部１３０は、ユーザプロセス空間１０内のサーバプロセス１２から取得したパケットを優先度に応じてクラス分けし、クラス別出力キュー１０３に設定する。暗号化されたパケットのクラス分けの処理については後述する。最初に入力に関する動作について説明する。
【００２６】図２は、本発明の入力動作のフローチャートである。
【００２７】ステップ１０１）　入力クラス分け部１１０において、ネットワークインタフェース２０からパケットを取得する。
【００２８】ステップ１０２）　入力クラス分け部１１０は、受け取ったパケットを優先度に応じて入力キューに分別する。このとき、暗号化されたパケットを受け取った場合の処理については後述する。
【００２９】ステップ１０３）　次に、パケット処理部１２０において、担当するキューに入れられたパケットの処理を行う。各処理は、それぞれに割り当てられたＣＰＵ数までの範囲の並列度で処理を行う。パケット処理のＣＰＵ数の制限方法については後述する。場合によっては、ユーザプロセス空間１０の暗号処理プロセスに暗号処理を引き渡し、処理してもらう。
【００３０】ステップ１０４）　入力キュー１０２を介して、ユーザプロセス空間１０の各プロセス（サーバプロセス１２または、暗号プロセス）に渡される。
【００３１】ステップ１０５）　各サーバプロセス１２は、通常のＯＳのプロセススケジューリングに備えられた機能により、優先度制御が行われる。サーバプロセス１２の優先度制御に関しては後述する。
【００３２】次に、出力動作について説明する。
【００３３】図３は、本発明の出力動作のフローチャートである。
【００３４】ステップ２０１）　ユーザプロセス空間１０の各サーバプロセス１２は、通常のＯＳのプロセススケジューリングに備えられた機能により、優先度制御が行われる。優先度制御されたパケットを出力クラス分け部１３０に転送する。なお、サーバプロセス１２の優先度制御に関しては後述する。
【００３５】ステップ２０２）　出力クラス分け部１３０は、サーバプロセス１２から送り出されたパケットは、クラス分け処理により優先度に応じた出力キューに分別され、クラス分け出力キュー１０３に設定される。暗号化されたパケットのクラス分け方法に関しては、後述する。
【００３６】ステップ２０３）　パケット処理部１２０は、該当するクラス別出力キュー１０３に設定されたパケットの処理を行う。各処理は、それぞれに割り当てられたＣＰＵ数までの範囲の並列度に基づいて処理を行う。パケット処理のＣＰＵ数の制限方法については後述する。場合によっては、ユーザプロセス空間１０の暗号処理プロセスに暗号処理を引き渡し、処理してもらう。
【００３７】ステップ２０４）　パケット処理が終わったパケットは、出力キュー１０４に設定され、ネットワークインタフェース２０を介して出力される。
【００３８】
【実施例】以下、図面と共に本発明の実施例を説明する。
【００３９】以下の実施例では、まず、８つのＣＰＵを備えた計算機を用いて、ＩＰｓｅｃによる暗号化通信を用いて、３つのサービスを提供する場合を例にして説明を行う。
【００４０】それぞれのサービスは、主に、ユーザプロセス空間のサーバプロセス１２とカーネル１００内におけるパケット処理部１２０により行われる。３つのサービスをサービスＡ，サービスＢ，サービスＣとする。
【００４１】本実施例における前提条件は以下の通りである。
【００４２】図４は、本発明の一実施例のサービス品質制御装置の構成を示す。－サービスＡのユーザプロセス空間におけるサーバプロセス１２は、『サーバプロセスａ』であり、優先度は『低』である。－サービスＢのユーザプロセス空間におけるサーバプロセス１２は、『サーバプロセスｂ』であり、優先度は『中』である。－サービスＣのユーザプロセス空間におけるサーバプロセス１２は、『サーバプロセスｃ』であり、優先度は『高』である。－サービスＡのカーネル１００内の処理は、『パケット処理ａ』によって行われ、優先度は『低』である。パケット処理ａの暗号処理は、『暗号処理プロセ

スｄ』を用いて行われる。ーサービスＢのカーネル１００内の処理は、『パケット処理ｂ』によって行われ、優先度は『中』である。ーサービスｃのカーネル１００内の処理は、『パケット処理ｃ』によってによって行われ、優先度は『高』である。ーカーネル１００内の処理に関して、それぞれパケット処理ａには１つ、パケット処理ｂには２つ、パケット処理ｃには３つまでＣＰＵが制限されている。

【００４３】以下に、具体的な実現方法に関して説明する。

【００４４】①　クラス分け方法：入力クラス分け部１１０及び出力クラス分け部１３０におけるクラス分け方法を以下に示す。

【００４５】ＩＰｓｅｃによる通信では、暗号鍵や復号鍵などの情報をＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）と呼ばれる情報として保持する。各パケット毎にこのＳＡをソースアドレス、ディスティネーションアドレス、ＳＰＩなどから探索し、暗号化や復号化処理を行う。このＳＡに優先度情報を記述しておく。

【００４６】図５は、本発明の一実施例のクラス分けを説明するための図である。

【００４７】入力クラス分け部１１０、出力クラス分け部１３０は、同図に示すように、パケット分類部１１１、メータリング部１１２、マーキング部１１３、シェーピング部１１４、及びキュー管理部１１５から構成される。

【００４８】クラス分け処理方法（入力クラス分け部１１０、出力クラス分け部１３０における処理）は、通常ＱｏＳルータのパケットフォーワードと同様の方法により行う。図５のように、まず、パケット分類部１１１において、上記のようにＳＡの探索を行い、そのＳＡにある優先度情報を元に、マーキング部１１３においてパケットに優先度情報を書き込む。それと同時に、メータリング部１１２において、優先度クラス毎にトラフィックの観測をしており、過剰なトラフィックが流れる場合には、シェーピング部１１４においてパケットの破棄、もしくは、マーキング部１１３において、優先度を下げたマークを付与するなどの処理を行う。その後に、キュー管理部１１５において、各優先度に合わせたキューに入れられる。

【００４９】②　ＣＰＵ数の制限方法：パケット処理部１２０において、それぞれ利用可能なＣＰＵ数を制限しておく。この制限方法は、当該パケット処理部１２０が起こせるスレッドの数を制限することにより実現する。具体的には、現在実行中のスレッド数を表す変数を用意しておき、その数が限度を超えたら空くまで処理を止めるという方法による。

【００５０】③　サーバプロセス１２の優先度制御：ユーザプロセス空間１０におけるサーバプロセス１２の優先度制御は、通常のＯＳに用意されている優先度制御方法を試用する。ＵＮＩＸ（登録商標）の場合では、ｎｉｃｅ値により、優先度制御を行う。

【００５１】④　ユーザプロセス空間１０における暗号処理プロセスによる処理：カーネル１００内のパケット処理部１２０からユーザプロセス空間１０へ暗号化もしくは、復号化するパケットを引き渡す。そして、カーネル空間より優先度の低いユーザプロセス空間において、しかもｎｉｃｅによりユーザプロセス空間１０においても優先度が付与された状態で、パケットの暗号処理を行う。処理を終えたパケットは、再びカーネル１００内部のパケット処理部１２０に戻す。

【００５２】また、上記の実施例は、図４に基づいて説明したが、カーネル内のクラス分け部１１０、１３０及びパケット処理部１２０の処理をプログラムとして構築し、サービス品質制御装置として利用されるコンピュータに接続されるディスク装置や、フロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現することが可能である。

【００５３】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

【００５４】

【発明の効果】上述のように、本発明によれば、ＯＳにおいて、ユーザプロセス空間のサーバプロセスとカーネル空間におけるパケット処理を割り当てるＣＰＵ数を制限すること、及び本来、カーネル内部で行う処理をユーザプロセス空間における暗号処理プロセスを用いることにより、サービス品質を制御することにより、暗号化通信によるセキュアかつリアルタイムなどのサービスの品質を保証した通信サービスを提供する場合に有効である。例えば、ＮＴＰのような時刻配送サービスと、ファイル転送サービスの両者を暗号化通信により提供する場合などである。

【００５５】今後は、インターネットにおいてセキュリティを考慮することは当然のこととなり、ＩＰｓｅｃがその標準として使われることが予想される。従って、そのような場合において、本発明のようなサービス品質制御は重要になることが予想される。

【図面の簡単な説明】

【図１】本発明のサービス品質制御装置の構成図である。

【図２】本発明の入力動作のフローチャートである。

【図３】本発明の出力動作のフローチャートである。

【図４】本発明の一実施例のサービス品質制御装置の構成図である。

【図５】本発明の一実施例のクラス分けを説明するための図である。

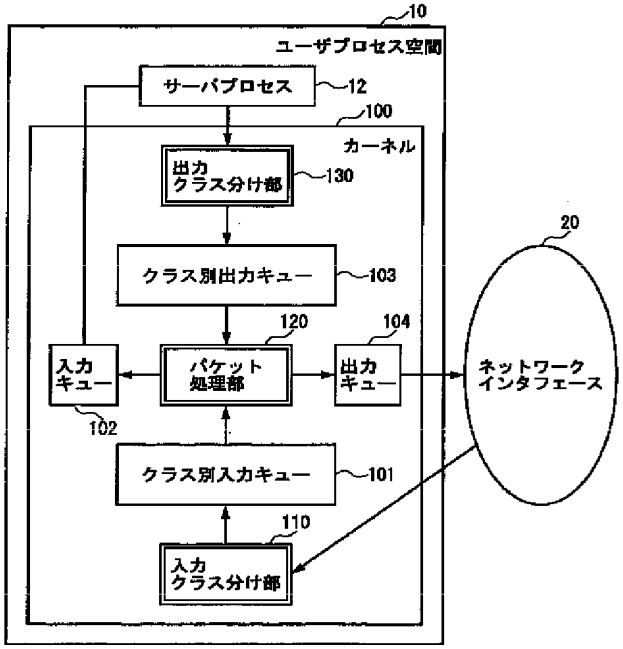
【符号の説明】

１０　ユーザプロセス空間

１２　サーバプロセス
２０　ネットワークインタフェース
１００　カーネル
１０１　クラス別入力キュー
１０２　入力キュー
１０３　クラス別出力キュー
１０４　出力キュー
１１０　入力クラス分け部
１１１　パケット分類部
１１２　メーリング部
１１３　マーキング部
１１４　シェーピング部
１１５　キュー管理部
１２０　パケット処理部
１３０　出力クラス分け部

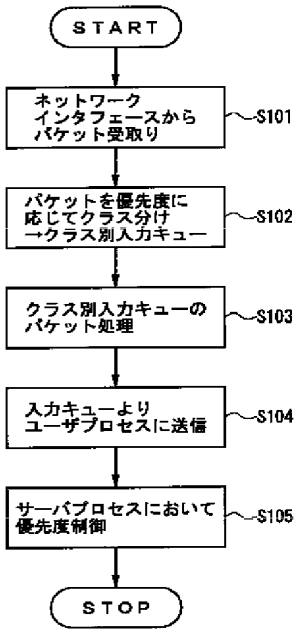
【図１】

本発明のサービス品質制御装置の構成図



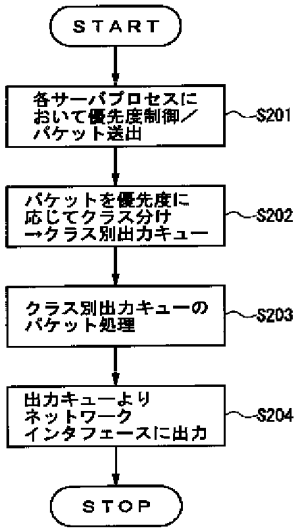
【図２】

本発明の入力動作のフローチャート



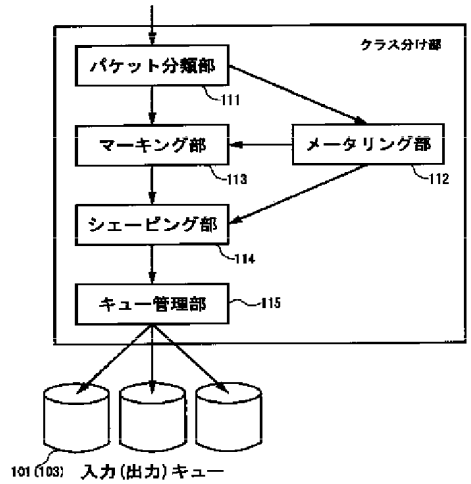
【図３】

本発明の出力動作のフローチャート



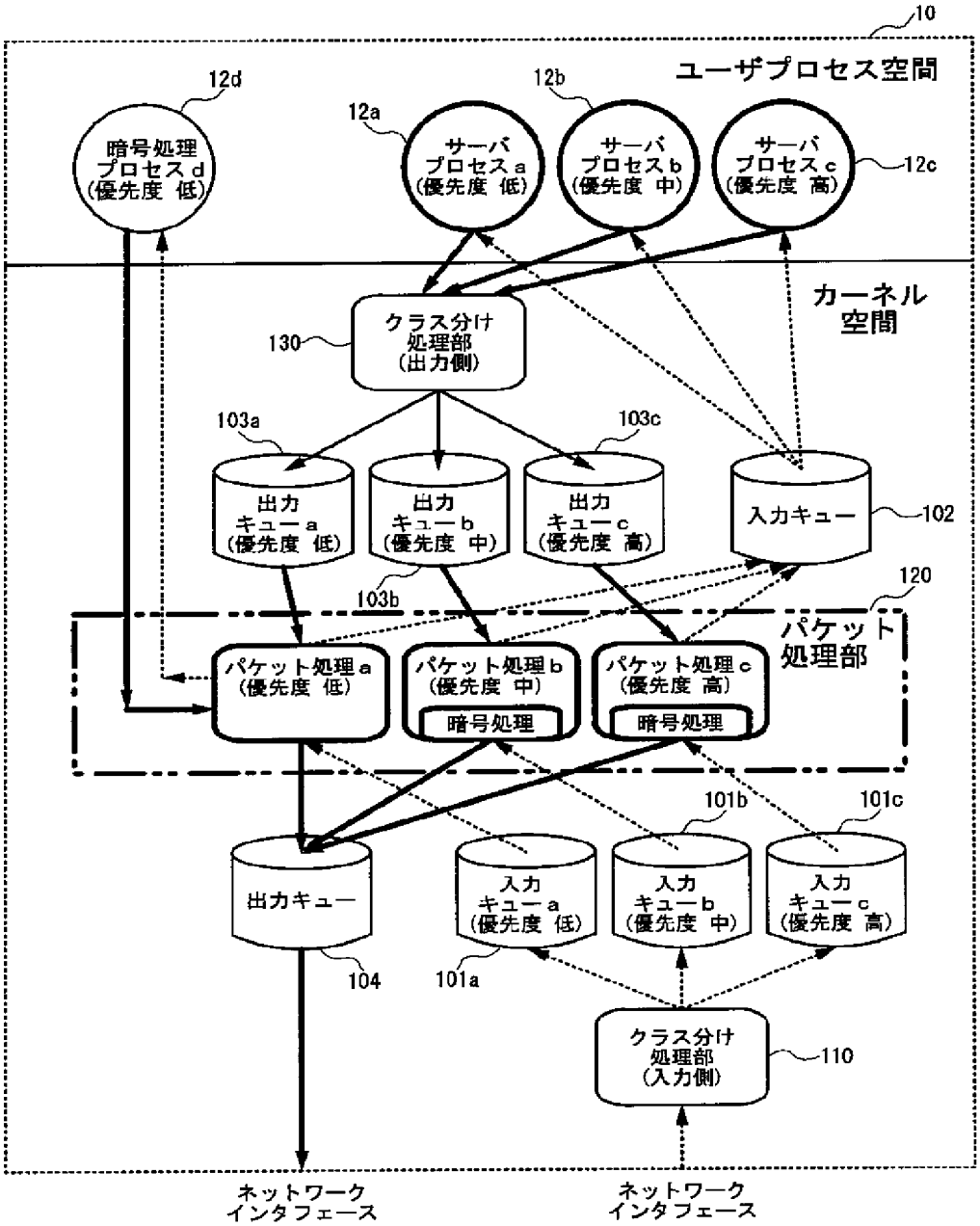
【図５】

本発明の一実施例のクラス分けを説明するための図



【図４】

本発明の一実施例のサービス品質制御装置の構成図



フロントページの続き

Ｆターム(参考)　5B045 BB28 BB42 BB47 EE12 EE29
GG09
5J104 AA32 PA07
5K030 GA15 HA08 HB17 LE05